Computer Security for I&C Systems at Nuclear Facilities

Michael T. Rowland, Donald D. Dudenhoeffer, and J. Scott Purvis
Division of Nuclear Security, Department of Nuclear Safety and Security
International Atomic Energy Agency
Vienna International Centre,
PO Box 100, 1400 Vienna, Austria
m.t.rowland@iaea.org; d.dudenhoeffer@iaea.org; s.purvis@iaea.org

ABSTRACT

Cyber-attacks on Instrumentation and Control (I&C) systems may jeopardize the safety and security of nuclear facilities by contributing to sabotage or aiding in the unauthorized removal of nuclear material. The effects of cyber-attacks on I&C systems important to safety to safety may result in a wide range of consequences, such as a temporary loss of process control or unacceptable radiological consequences. Public awareness of cyber-attacks that affect I&C systems may also undermine confidence in the safety and security of nuclear facilities.

The International Atomic Energy Agency (IAEA) recognizes the need for the guidance on the protection of I&C systems that provide safety, security, or auxiliary functions at nuclear facilities from cyber-attacks. To meet this need, The IAEA has developed a new Nuclear Security Series publication with the provisional title *Computer Security of Instrumentation and Control Systems at Nuclear Facilities* which builds upon and expands the guidance published in Nuclear Security Series No. 17 *Computer Security at Nuclear Facilities* (2011) [1]. This publication will be formally released in 2017 as Technical Guidance and will be the second international consensus publication dedicated to Computer Security at Nuclear Facilities. It was developed in parallel with the new IAEA Nuclear Safety publications providing recommendations on I&C systems at research reactors (RR) [2] and nuclear power plants (NPP) [3].

The purpose of this paper is to provide an overview of this publication and its application. The paper will also discuss its relation to other IAEA Nuclear Security Series (NSS) publications on computer security.

Key Words: Nuclear Security, Computer Security, Cyber Security, I&C.

1 INTRODUCTION

Protection of computer-based systems (including digital I&C systems) is recommended by the Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [4], paragraph 4.10, which states that "computer based systems used for physical protection, nuclear safety and nuclear material accountancy and control should be protected against compromise (e.g. cyber-attack, manipulation or falsification) consistent with the threat assessment or design basis threat". This same requirement is often used as a basis for national computer security regulation for nuclear facilities.

The increasing use of digital technology within nuclear facilities has changed the nature of I&C systems and has enabled the interconnection of remotely or locally reprogrammable and functionally distinct I&C systems. The use of commercial off-the-shelf technologies and standard protocols means that these I&C systems have inherited the vulnerabilities associated with these technologies. New designs must now consider the application of computer measures to assure their security. This need is further confirmed by the public disclosure of several computer security incidents including targeted attacks at nuclear facilities over the past decade.

The scope of the forthcoming publication titled *Computer Security of I&C systems at Nuclear Facilities* (NST036), is the application of computer security measures to I&C systems that provide safety, security, or auxiliary functions at nuclear facilities. These measures are intended to protect I&C systems against malicious acts perpetrated by individuals or organizations. This publication also addresses the application of such measures throughout the lifecycle of these systems. This includes the development, simulation and maintenance environments of these systems.

2 IAEA NUCLEAR SECURITY SERIES PUBLICATIONS AND COMPUTER SECURITY

Since 2006, the IAEA has issued NSS publications [5] to assist Member States (MS) in establishing effective national nuclear security regimes. These publications complement international legal instruments on nuclear security, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council Resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources. Guidance from the NSS can be used voluntarily by MS in the development of their national policy, regulations, and security plans.

The NSS publications are not authored by the IAEA directly, but are developed by international experts. Since 2012, the Director General of the IAEA has created the Nuclear Security Guidance Committee (NSGC) with the remit to its terms of reference [6]. The development process for a new publication normally takes three to four years. A structured review process consisting of internal committees and external Member State reviews results in consensus approval of the final document. It is important to stress that these documents are the product of Member State subject matter experts and require consensus agreement for release. This process has many similarities with the IAEA Safety Standards Series process and often interacts with the same review committees.

The NSS publications are arranged within a structured tiered series of four levels. The multiple tiers of publications as shown in Figure 1 are:

Figure 1: Tiers of Nuclear Security Series Publications

Nuclear Security Fundamentals specify the objective of a State's nuclear security regime and the essential elements of such a regime. These provide the basis for the Nuclear Security Recommendations. A single publication, *Nuclear Security Series No. 20 Objective and Essential Elements of a State's Nuclear Security Regime (NSS20)* [7], exists at this level.

Nuclear Security Recommendations publications set out measures that MS should take to achieve and maintain an effective national nuclear security regime consistent with the Fundamentals. Three publications exist at this level:

- *NSS No. 13 Nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/Revision 5)* (NSS13) [4];
- *NSS No. 14 Nuclear security recommendations on radioactive material and associated facilities* (NSS14) [8];
- *NSS No. 15 Nuclear security recommendations on nuclear and other radioactive material out of regulatory control* (NSS15) [9].

Implementing Guides provide guidance on means by which MS could implement the measures set out in the Recommendations. As such, they focus on how to meet the Recommendations relating to broad

areas of nuclear security. The IAEA has published a single implementing guide related to information security, *NSS No. 23-G Security of Nuclear Information* [10]. A second publication dedicated to computer security is currently in development, *NST045* with the provisional title *Computer Security for Nuclear Security*.

Technical Guidance publications provide guidance on specific technical subjects to supplement the guidance set out in Implementing Guides. They focus on details of how to apply the necessary security measures. The IAEA published NSS17 [1] in 2011.

Table I provides a summary of draft NSS publications currently under development that focus on computer security:

Document	Status
NSS Technical Guidance *NST036 Computer Security of I&C Systems at Nuclear Facilities.* - Provides guidance on implementing computer security controls across the life cycle of nuclear instrumentation and control systems.	Publication in 2017
NSS Implementing Guide *NST045 Computer Security for Nuclear Security.* - Provides overarching guidance to assist Member States in implementing computer security as a part of their nuclear security regime.	Completed 120-day Member State (MS) Review April 2017
NSS Technical Guidance *NST047 Computer Security Techniques for Nuclear Facilities*. - Provides discussion on good practices for implementing computer security associated digital technologies at nuclear facilities.	To be submitted to NSGC (June 2017) Request to proceed to 120-day MS Review

Table I: Draft NSS computer security publications

2.1 Relationship of NSS Publications to Safety Standards Series

Safety design considerations play a large role in the development of nuclear instrumentation and controls systems. The IAEA provides the Safety Standards Series as a framework of guidance publications to support MS implementation of nuclear safety.

The recently published specific safety guides SSG-37 [2] and SSG-39 [3] provide recommendations on the design of instrumentation and control (I&C) systems to meet the requirements established in the Specific Safety Requirements. The objective of these Safety Guides is to provide guidance on the overall I&C architecture and on I&C systems important to safety at Research Reactors (RR) [2] and Nuclear Power Plants (NPP) [3] to ensure safe operation of these facilities.

Additionally, SSG-39 [3] and NST036 contain guidance that was co-authored and therefore these documents are strongly aligned. The guidance found within the 'Computer Security' section of SSG-39 [3] is related to the guidance found within the 'Safety Considerations for Computer Security Measures' of NST036.

Paragraph 3.48 of NST036 resulted in extensive discussions with the NSGC regarding whether the guidance allowed for an absence of a security solution in cases where the proposed measures were in conflict with safety design considerations. While the previous draft text to this paragraph was taken directly from paragraph 7.103 in SSG-39 [3], there was a failure to come to a general agreement within the NSGC that this text was appropriate. The NSGC was concerned that, without changes to the text, serious deficiencies in computer security could be "justified" and "accepted".

This concern was resolved by changing the final two sentences in paragraph 3.48 of NST036 to ensure that security considerations were addressed. This approved text states:

> *"If there is a conflict between safety and security, then design considerations taken to assure safety should be maintained provided that the operator seeks a compatible solution to meet computer security requirements. Compensatory computer security measures should be implemented to reduce the risk to an acceptable level and be supported by a comprehensive justification and security risk analysis. The implemented measures should not rely solely upon administrative control measures for an extended period. The absence of a security solution should never be accepted."*

The approved text now emphasizes that the absence of security solution should never be accepted. This emphasis differs from SSG-39 [3], which "strongly discourage[s]" the absence of a security solution. The change was seen by the NSGC as necessary to ensure security considerations were properly reflected within the security focused NSS Publications.

2.2 The Relation of NSS Publications to International Standards

NSS publications represent a level of guidance for Member States in developing and implementing nuclear security (including computer security), but they are not international standards. NSS publications serve to inform the development of standards. Since 1977, the IAEA has had a cooperation agreement with the International Electrotechnical Commission (IEC), specifically with IEC/SC45A Instrumentation and control of nuclear facilities. In 2014, this agreement was expanded to include collaboration in nuclear security.

The IAEA has also strengthened its collaboration with the United Nations standards body, the International Telecommunication Union (ITU), to identity complementary areas and possible opportunities to jointly support Member State's development of computer security programs. It must again be noted that the Division of Nuclear Security's (NSNS) focus on computer security is as a component of nuclear security. Computer security for the nuclear sector is not covered by any other United Nations organization.

3 KEY CONCEPTS OF THE PUBLICATION

The intended audience for the new publication includes competent authorities, including regulatory bodies, as well as nuclear facility management, operations, maintenance and engineering personnel, I&C vendors, I&C designers, research laboratories and other organizations concerned with the safety and security of nuclear facilities. Nuclear facilities include, but are not limited to:

- Nuclear Power Plants (NPP)
- Nuclear Research Reactor (RR) Facilities
- Nuclear Fuel Cycle Facilities (FCF)
- Nuclear and Radioactive Waste Storage Facilities

3.1 Computer Based Systems and I&C Systems

'Computer-based systems' providing specific functions are explicitly referred to in NSS13 [4] as requiring protection from cyber-attack. Since the publication of NSS13 [4] in 2011, the terminology has continued to evolve where the term 'computer-based systems' has equivalence to the term 'digital technologies'. All items covered under the terms 'computer-based systems' and 'digital technologies' are susceptible to cyber-attacks (e.g. electronic means of compromise) and demand the application of computer security measures to ensure that their confidentiality, integrity, and availability requirements are met.

These digital technologies are ubiquitous in modern day society, and therefore there is a need to define terms that would clearly demarcate the nuclear security regime and specifically those systems having importance to nuclear safety and security. The term 'I&C System' in NST036, refers to those instrumentation and control systems that make use of, depend upon or are supported by digital technologies and therefore are susceptible to cyber-attack.

3.2 Risk Informed Approaches

NSS20 [7] states that "A nuclear security regime uses risk informed approaches". According to NSS20 [7], these risk informed approaches take into account (1) the State's current assessment of threat, (2) attractiveness and vulnerability of targets, (3) characteristics of the targets, and (4) potential harmful consequences.

A risk-informed approach to computer security for I&C systems may use risk assessments to identify the facility's vulnerabilities to cyber-attack related to these systems and determine the consequences that could result from the successful exploitation of these vulnerabilities. Computer security measures should be assigned based on the results of the risk assessments.

NST036 identifies two distinct types of risk assessments, which are (1) Facility Computer Security Risk Assessment (FCSRA) and (2) System Computer Security Risk Assessment (SCSRA).

The FCSRA is used to identify the facility's vulnerabilities to cyber-attack and to determine the consequences that could result from the successful exploitation of these vulnerabilities, including those in I&C systems. The FCSRA would consider the entire facility and provide an assessment of the aggregate risk.

The SCSRA determines the security risk posed by cyber-attacks on individual or multiple I&C systems, subsystems or components. The SCSRA would consider a single system or subset of systems. The expectation is that for each FCSRA there would be many SCSRAs.

I&C systems are often essential for facility safety, consequently an understanding of nuclear safety can assist in assessing risk, developing computer security measures for the I&C system, assessing potential conflicts between safety and security, and determining how such conflicts could be resolved. For example, adversaries could sabotage a facility through a cyber-attack on the facility's I&C systems, resulting in potential safety and security consequences. Such attacks might cause failures of I&C systems or might cause I&C systems to operate in ways that differ from their intended behaviour or their analysed failure modes.

3.3 I&C Life Cycle Models

The development of *NST036 Computer Security of I&C Systems at Nuclear Facilities* was aligned closely with the SSG-37 [2] and SSG-39 [3]. This alignment included the use of the I&C life cycle model to structure the guidance in both NST036 and SSG-39 [3]. The intent of this parallel structure is to simplify the safety-security interface as with respect to the published guidance, thereby easing the implementation of both the safety and security considerations.

Another goal of using the I&C life cycle model is to promote the integrated implementation of safety and security measures. Through integration, these measures become mutually supportive resulting in systems that are more resilient system to both malicious and non-malicious acts with the potential to result in unacceptable radiological consequences. By identifying computer security considerations at the appropriate life cycle stage, the potential measures that may be implemented are significantly increased in number, type, and effectiveness. For example, specification of application whitelisting at the system requirements phase would allow for the measure to be included within all verification and validation activities necessary for safety and security. This would minimize duplication of effort and has the

potential to enhance effectiveness by ensuring that all applications and services are limited to only those required by the system.

3.4 Safety-Security Interface

The fundamental objective of both nuclear safety and nuclear security is to protect people and the environment from harmful effects of ionizing radiation. Nuclear Safety addresses this from the view of protection from natural hazards, system failure and human error. Nuclear Security addresses this principle from the aspect of protection from and mitigation of malicious acts. Safety and security share many common elements but there are also challenges related to differences in approach and culture between the two disciplines [11]. These challenges are of primary concern when selecting computer security measures to apply to the design and operation of instrumentation and control systems in nuclear facilities. Therefore, the interface between safety and security needs to be well defined to ensure its effectiveness in balancing safety and security design considerations.

Another key difference between safety and security considerations is the concept of defence in depth. The term "safety defence in depth" is used in this publication to refer to defence in depth as defined in the IAEA Safety Glossary [12] as:

> "A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions."

Further, the IAEA Fundamental Safety Principles (SF-1) [13] discusses the implementation of defence in depth concept "through a combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment."

The Safety Standard, Safety of Nuclear Power Plants: Design [14] provides additional explanation of concept of defence in depth for Nuclear Power Plants that includes the guidance on the purpose of each of the five levels of defence in depth.

This is similar to the security-focused concept of defence in depth as defined in NSS 20 [7] as "The combination of successive layers of nuclear security systems and nuclear security measures for the protection of targets from nuclear security threats."

However, there are a few key differences between the safety and security concepts of defence in depth are (1) security emphasizes protection from nuclear security threats (i.e. a person or group of persons) and (2) safety emphasizes independent levels of protection.

Paragraph 3.2 of SF-1 [13] states that "safety is concerned with both radiation risks under normal circumstances and radiation risks as a consequence of incidents[1]." However, paragraph 1.10 of SF-1 [13] limits the safety principles application to security to (1) provisions in design and construction, (2) controls on access to prevent theft of categorized material, (3) mitigations of the consequences of accidents and failures resultant from breaches in security, and (4) security measures with respect to management of radioactive sources and material. This eliminates any considerations or provisions for the actions of the malicious threat actor (i.e. nuclear security threat) in the design and implementation of nuclear security systems and measures which deter, detect, delay and respond to unauthorized malicious acts. However, by excluding this consideration of the threat actor, the safety analysis is bounded.

[1] Incidents' includes initiating events, accident precursors, near misses, accidents and unauthorized acts (including malicious acts and non-malicious acts)."

This differs from the nuclear security perspective, which must consider human adversaries, who adapt and evolve their tactics, techniques, and procedures (TTP) to continually attempt to overcome the security of facilities (and their respective nuclear security system). Security relies upon a threat assessment or threat model that bounds the analysis. The quality of the threat assessment degrades with the passing of time because the threat is constantly changing, and therefore it must be periodically updated. This is particularly important when assessing threats having cyber skills, since their TTPs change rapidly.

The rapidly evolving TTP of the cyber adversary therefore demands application of computer security measures that can be adapted in order to continue to provide adequate protection. Therefore, it should be acknowledged that the security analysis is bounded to the threat assessment and thus the design of system and measures to address the threat should consider the potential that sequential assessments will be significantly different from one another.

4 IMPLEMENTATION OF COMPUTER SECURITY FOR I&C SYSTEMS

4.1 Application of a Graded Approach

NST036 recommends that computer security measures be based upon a risk informed, graded approach, which takes into account the following:

- The importance of I&C system functions for both safety and security;
- The identified and assessed threats to the facility;
- The attractiveness of the I&C system to potential adversaries;
- The vulnerabilities of the I&C system;
- The operating environment; and
- The potential consequences that could either directly or indirectly result from a compromise of the I&C system functions.

NST036 provides a priority for assigning computer security measures when considering the potential consequences to the system (i.e. not the facility). NST036 paragraph 2.19 states "The potential consequences of a compromise on I&C system function are, arranged from worst to best cases:

- The function is indeterminate. The effects of the compromise result in an unobserved alteration to system design or function;
- The function has unexpected behaviours or actions which are observable to the operator;
- The function fails; or
- The function performs as expected, meaning the compromise does not adversely affect system function (i.e. fault tolerant)."

This priority provides significant insight when accrediting the specific safety analysis or features with the provision of a security benefit. It is not common for safety analysis to consider incidents when the function is indeterminate, or where it operates in a way inconsistent with or contradictory to its design basis for safety. For example, cyber-attacks can compromise a supporting system in such a manner that the supporting system attacks the system which it was previously supporting.

An important aspect of NST036 that assists the reader in interpreting and applying the guidance is the statement of scope in the first paragraph in many of the sections. For example, the section pertaining to secure development environments begins with paragraph 4.32, which states:

"The guidance contained within this section applies to the development of all I&C systems, subsystems and components to which a graded approach to computer security is applied in accordance with their assigned security level."

This paragraph sets the scope of the guidance as "development of all I&C systems" and also provides text to guide the level of adherence "a graded approach … in accordance with their assigned security level." Therefore, the guidance is to be applied to all development environments; however, the level of effort and/or resources to be applied should consider the security level assigned to that system. The first paragraph in each section is critical to ensuring that limited resources for computer security are applied based upon a graded approach resulting in effective risk reduction and management.

4.2 Computer Security Measures

Computer security measures are used to prevent, detect, delay, and respond to malicious acts and to mitigate the consequences of such acts. Computer security measures are also used to ensure that non-malicious acts do not degrade security or increase the vulnerability of computer-based systems to malicious acts.

Within NST036, computer security measures that address vulnerabilities in the system or provide protective layers of defence are assigned to one of three categories: (1) technical control measures, (2) physical control measures or (3) administrative control measures. When developing integrated computer security for I&C systems, NST036 recommends that all three categories should be considered and an appropriate combination selected.

Technical control measures are hardware and software used to prevent, detect, mitigate the consequences of and recover from an intrusion or other malicious act. The ability of technical control measures to provide continuous and automatic protective actions is significant when considering their effectiveness compared to physical or administrative control measures.

Physical control measures are physical barriers that protect instruments, computer-based systems and supporting assets from physical damage and unauthorized physical access. Physical control measures include locks, physical encasements, tamper indicating devices, isolation rooms, gates and guards.

Administrative control measures are policies, procedures and practices designed to protect computer-based systems by providing instructions for actions of employees and third party personnel. Administrative control measures specify permitted, necessary and forbidden actions by employees and third party personnel. Administrative control measures for nuclear facilities include operational and management control measures.

4.3 Security Levels and Zones

Computer security in nuclear facilities is commonly implemented and constructed using computer security levels and zones. The IAEA first introduced the use of computer security levels and zones was in NSS17 [1] which includes an example implementation at a NPP.

Computer security levels[2] are values assigned to each I&C system in a facility to indicate the degree of computer security protection required. Each level will need different sets of computer security measures to

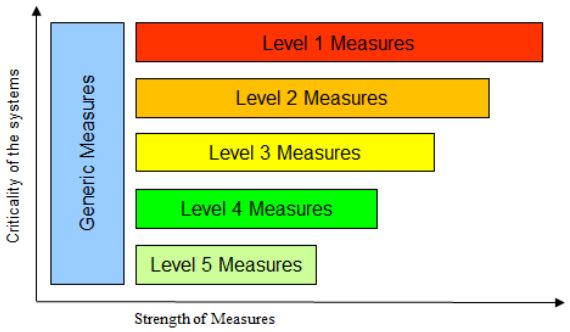

Figure 2 Level of security/strength of measures

[2] Computer security levels and safety classes are distinct but related concepts. The safety classification of an item important to safety is based upon the relevance to safety of its function as well as potential consequences of its failure.

satisfy relevant computer security requirements. Figure 2 illustrates an example involving 5 security levels ranging from level 5 (least protection needed) to level 1 (most protection needed).

The security zone concept involves the logical and/or physical grouping of computer-based systems that share common computer security requirements, due to inherent properties of the systems or their connections to other systems. All systems located within a single zone are protected at the same security level, namely that assigned to the system with the most stringent security level within the zone. Grouping of I&C systems into zones may simplify the application and management of computer security measures. Note that the numbering the levels is just the opposite of the number scheme presented in the USNRC Regulatory Guide 5.71.

5 CONCLUSIONS

This paper has presented the draft publication IAEA NST036 *Computer Security of Instrumentation and Control Systems at Nuclear Facilities* that is to be published in 2017. This publication considers the following main topics:

- Expansion upon the guidance published in Nuclear Security Series No. 17 Computer Security at Nuclear Facilities (2011) [1].
- The Safety and Security interface, specifically the coherence between the safety guides (SSG-37 [2] and SSG-39 [3]) and other NSS publications while accounting for the different intended audience.
- The key concepts detailed in the publication such as risk informed approaches, defence in depth and graded approach principles, FCSRA, SCSRA, and specific computer security considerations for I&C systems at nuclear facilities.
- The structure of the publication aligning with the I&C lifecycle model as being central to the interpretation of the guidance.

The final draft of NST036 and other materials including expert meeting reports, draft documents, and training materials are openly available on the NUSEC portal (https://nusec.iaea.org/portal/). While entry to the portal is controlled, nuclear security professionals including those in computer security are encouraged to register for access.

6 ACKNOWLEDGMENTS

The IAEA Division of Nuclear Security Computer Security programme is the reflection of the input from Member States and international experts. This programme is very much driven by Member State needs and priorities, and will continue to adapt to address those needs.

7 REFERENCES

1. International Atomic Energy Agency, *IAEA Nuclear Security Series No. 17,Computer Security at Nuclear Facilities*, Technical Guidance, IAEA, Vienna (2011)
2. International Atomic Energy Agency, *IAEA Safety Standards Series No. SSG-37, Instrumentation and Control Systems and Software Important to Safety for Research Reactors,* Specific Safety Guide, IAEA, Vienna (2015)
3. International Atomic Energy Agency, *IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants,* Specific Safety Guide, IAEA, Vienna (2016)

4. International Atomic Energy Agency, *IAEA Nuclear Security Series No. 13*, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5),* Nuclear Security Recommendations, IAEA, Vienna (2011)
5. International Atomic Energy Agency, "IAEA Nuclear Security Series", http://www-ns.iaea.org/security/nuclear_security_series.asp, (2014).
6. International Atomic Energy Agency, "Terms Of Reference for The Nuclear Security Guidance Committee", (2012).
7. International Atomic Energy Agency, *IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime,* Nuclear Security Fundamentals, IAEA, Vienna (2013)
8. International Atomic Energy Agency, *IAEA Nuclear Security Series No. 14*, *Nuclear Security Recommendations on Radioactive Material and Associated Facilities,* Nuclear Security Recommendations, IAEA, Vienna (2011)
9. International Atomic Energy Agency, *IAEA Nuclear Security Series No. 15*, *Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control,* Nuclear Security Recommendations, IAEA, Vienna (2011)
10. International Atomic Energy Agency, *IAEA Nuclear Security Series No. 23-G,Computer Security at Nuclear Facilities*, Implementing Guide, IAEA, Vienna (2015)
11. International Atomic Energy Agency, *IAEA INSAG-24, The Interface Between Safety and Security at Nuclear Power Plants*, Report by International Nuclear Safety Group, IAEA, Vienna (2010)
12. International Atomic Energy Agency, "IAE Safety Glossary 2016 Revision" https://www-ns.iaea.org/downloads/standards/glossary/iaea-safety-glossary-rev2016.pdf, IAEA, Vienna (2016)
13. International Atomic Energy Agency, *IAEA Safety Standards No. SF-1, Fundamental Safety Principles,* Safety Fundamentals, IAEA, Vienna (2006)
14. International Atomic Energy Agency, *IAEA Safety Standards No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design,* Specific Safety Requirements, IAEA, Vienna (2016)